To ensure the safety of wireless technology in a control system environment, INL's John Buttles has designed a wireless sensor test bed to investigate the behavior of different wireless devices.

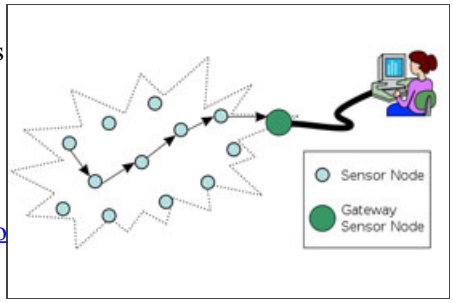
Wireless sensor test bed to provide guidelines for industrial systems

By Ryan Weeks, *INL Communications and Governmental Affairs*

For many companies, installing wireless technology inside factories, power plants and nuclear facilities can be risky. Although wireless is cheaper than cable connections, the flow of information is not as reliable.

That may not be a big deal when you're surfing the Net at home, but at a factory or power plant with automated control systems, even a five-second disruption could have serious consequences.

"A malfunction could cause a water tower to overflow," said John Buttles, a senior engineer at Idaho National Laboratory. "Or you could end up with the wrong colored pill in a bottle instead of aspirin."



Wireless sensor networks are made up of several sensors or nodes that measure conditions and supply data to a control system.

Buttles is devising and testing wireless sensor networks (WSN) to help ensure the transition to wireless is safer for power plants, factories and other facilities with automated control systems. He is using INL's Center for Advanced Energy Studies to design a wireless sensor test bed where he can investigate vulnerabilities and weaknesses of these networks. CAES' wireless system, along with its laboratories and office space, provides an environment that is similar to an industrial setting.

Wireless sensors measure environmental conditions such as volume, temperature and pressure.

"We want to make sure these devices are put in correctly, and the CAES environment best resembles a real-world installation," Buttles said.

WSN are designed to help measure and manage the operation of an industrial control system. They are composed of a number of sensors or nodes that monitor environmental conditions such as temperature, pressure and volume. The nodes relay readings, known as sensory data, to a central point that connects to the control system, which then makes decisions based on the information.

Transmitting and receiving sensory data in a timely and consistent manner is key to keeping a control system running smoothly.

Buttles' hypothesis is that radio frequencies and cyber interferences can interrupt the flow of sensory data. Interferences that slow down, corrupt or even stop sensory data from reaching its destination can cause an entire control system to fail.

"And that is enough to ruin your day," he said.

At CAES, Buttles will monitor the effect that existing frequencies and interferences have on the networks he has installed. He also will operate multiple types of radio systems and generate interferences.

In addition, Buttles will collect data on different models and styles of wireless hardware. Multiple vendors design instruments with unique characteristics and protocols, and each design may have different rules that govern how messages are exchanged between devices. Buttles' research will mesh the different types of devices and determine the compatibility of each instrument.

Student researchers at CAES will then use software to simulate various settings and industrial environments. The researchers will create computer models of WSN behavior and predict their operation in different scenarios and conditions.

A gateway node is a central point that collects data from wireless sensors and

Buttles expects the research to establish design guidelines and standards — something the industry ***transmits it to the control system.*** currently lacks — which will benefit both vendors and customers. He also hopes his research will improve the resilience of wireless sensor networks and, more importantly, move industry one step closer to ensuring the safety of our nation's critical infrastructure control systems.

"That's what we do here — we figure out those tough problems that industries can not or do not want to," he said.

Feature Archive